FILED UNDER SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

[UNDER SEAL], **PLAINTIFF,** **v.** **[UNDER SEAL],** **DEFENDANTS**	No. 15 Civ. ____ **FILED UNDER SEAL**

DECLARATION OF KENNETH ZAVOW

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **v.** **ARKADIY DUBOVOY, et al.,** **Defendants.**	**Case No.**

Declaration of Kenneth Zavos

I, Kenneth Zavos, hereby declare as follows:

1. I am employed as an IT Forensics Analyst at the U.S. Securities and Exchange Commission's Division of Enforcement in Washington, D.C. As part of my duties I was asked to analyze and review the following:

a. forensic images taken of servers used by Newswire Service 1

b. documents and communications produced by the Federal Bureau of Investigation

c. forensic images taken of servers used by Newswire Service 2

d. reports of forensic exams conducted by Cybersecurity Company 1

e. information provided by Newswire Service 1 and Newswire Service 2

The Hacker Defendants Accessed Unpublished News Releases at Newswire Service 1

2. I reviewed reports of forensic exams conducted by Cybersecurity Company 1 regarding unauthorized computer intrusions at Newswire Service 1 that occurred from at least March 2010 until July 2014.

3. Those reports show that unauthorized individuals ("hackers") used Structured Query Language ("SQL") injections to gain access to Newswire Service 1's computer servers.

4. SQL is a computer programming language designed for managing data in a database system. Using SQL queries users can retrieve specifically-requested data from a given database. SQL injection is a technique computer hackers use to steal content from a computer network.

5. Cybersecurity Company 1 specifically determined:

a. The hackers used SQL injection to insert code into Newswire Service 1's network which gave the hackers access to Newswire Service 1's servers.

b. From March 2010 through July 2010, the hackers issued more than 2,300 discovery SQL queries and 23,000 SQL content requests to Newswire Service 1 servers, through which they extracted the content of not-yet-public press releases.

c. From August 2010 until November 2010, the hackers issued approximately 360 discovery SQL queries and 4,700 SQL content requests to Newswire Service 1 servers, through which they extracted the content of not-yet-public press releases.

d. From January 2011 until July 2011, the hackers issued approximately 4,200 discovery SQL requests and 34,300 SQL content requests to Newswire Service 1 servers, through which they extracted the content of not-yet-public press releases.

e. From July 2011 until March 2012, the hackers issued approximately 48 discovery SQL requests and 2,300 SQL content requests to Newswire Service 1 servers, through which they extracted the content of not-yet-public press releases.

11. In addition to providing the hackers' access, the malware installed by the hackers was designed to delete and conceal evidence of their activities. Despite the hackers' efforts to hide their activities, Newswire Service 2's logs recorded more than 55,000 instances of unauthorized press release extractions.

12. On January 12, 2011, Newswire Service 2's IT staff switched servers which had the unintentional effect of terminating the hackers' access to Newswire Service 2's server.

13. In March 2012, Newswire Service 2 hired Cybersecurity Company 2 to analyze and help protect Newswire Service 2's network from intrusions. In March 2012, Cybersecurity Company 2 determined that hackers were accessing Newswire Service 2's servers without authorization. In the course of that investigation, Cybersecurity Company 2 found, among other things, that malware installed on one of the servers was collecting and transmitting passwords from the organization to the hackers every five minutes. Additionally, Cybersecurity Company 2 also determined the hackers had installed malware on Newswire Service 2's servers that was intended to be used to conceal their hacking activity.

14. In January 2013, the hackers accessed Newswire Service 2's computer systems through compromised Virtual Private Network ("VPN") credentials. The use of an authorized user's VPN credentials allowed the hackers to conceal their intrusions. Newswire Service 2 discovered the use of compromised VPN credentials, and took steps to end the intrusions in March 2013.

Identification of the Hackers

15. The hackers used multiple IP addresses to attack Newswire Service 1 and/or Newswire Service 2' servers, including but not limited to IP addresses ending: *18.42; *9.101; *136.6, and *26.98.

16. I analyzed emails from a Google email account, which the FBI identified as belonging to defendant Ivan Turchnyov. The meta-data for Turchynov's email account shows he used a computer with the IP address ending *18.42 to access webpages in December 2011.

17. The IP address ending *18.42, originating in Ukraine, was used multiple times to hack both Newswire Service 1 and Newswire Service 2.

18. A video named "readme.avi" was sent as an attachment to an email from Turchnyov's account on October 25, 2010. This video depicts the unauthorized collection of information from Newswire Service 2's servers. This video shows:

a. A Windows' computer screen with a custom administrator panel.

b. The administrator panel is split into two parts - the "documents" section on the left and the "archives" section on the right.

c. The "documents" section contains a list of more than 300 file names with id numbers, and the "archives" section contains the names of zip archives. Many of the file names include the term "release" in the file name. The file id numbers match those used internally by Newswire Service 2 to identify press releases for publicly-traded companies.

d. The hacker uses Cyrillic to provide on-screen narration and to conduct the unauthorized intrusion depicted.

e. Ten files are selected in the administrator panel and downloaded into a zip archive, automatically named "24 Oct 1440.zip" after the Day, Month, and Time in 24-hour clock format.

f. The downloaded files are opened on screen, showing that they are press releases for publicly-traded companies.

Case 2:15-cv-06076-MCA-MAH Document 2-3 Filed 08/10/15 Page 6 of 7 PageID: 103

g. The IP address of the system being used in the operation is also clearly visible in the status bar of one window and the URL field of two other windows.

19. Newswire Service 2's server logs show they were accessed by hackers on October 24, 2010 by the same IP address depicted as downloading files to the "24 Oct 1440.zip" file referenced above. All of the files within the zip archives in the "24 Oct 1440.zip" file referenced above matched the entries in the Newswire Service 2 server log with respect to date, approximate time, file size, and IP address to which they were extracted.

I, Kenneth Zavos, do hereby declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct to the best of my knowledge. Executed on this 10th day of August, 2015.

Kenneth Zavos